UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

January 30, 2026

Ronald O. Mueller
Gibson, Dunn & Crutcher LLP

Re: Amazon.com, Inc. (the "Company")
Incoming Letter dated January 19, 2026

Dear Ronald O. Mueller:

This letter is in response to your correspondence concerning the shareholder proposal (the "Proposal") submitted to the Company by American Baptist Home Mission Society and co-filers for inclusion in the Company's proxy materials for its upcoming annual meeting of security holders.

The Company represents that it has a reasonable basis to exclude the Proposal. Based solely on that representation, we will not object if the Company excludes the Proposal from its proxy materials.

Copies of all of the correspondence on which this response is based will be made available on our website.

Sincerely,

Division of Corporation Finance
Office of Chief Counsel

cc: Aaron Acosta
Investor Advocates for Social Justice

GIBSON DUNN

Ronald O. Mueller
Partner
T: +1 202.955.8671
rmueller@gibsondunn.com

January 19, 2026

VIA ONLINE PORTAL SUBMISSION

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: *Amazon.com, Inc.*
Shareholder Proposal of American Baptist Home Mission Society et al.
Securities Exchange Act of 1934—Rule 14a-8

Ladies and Gentlemen:

This letter notifies the staff of the Division of Corporation Finance (the "Staff") that our client, Amazon.com, Inc. (the "Company"), intends to omit from its proxy statement and form of proxy for its 2026 Annual Meeting of Shareholders (collectively, the "2026 Proxy Materials") a shareholder proposal and statement in support thereof (collectively, the "Proposal") submitted by American Baptist Home Mission Society, as lead proponent (the "Lead Proponent") and numerous co-filers (collectively with the Lead Proponent, the "Proponents").

Pursuant to Rule 14a-8(j) and the Statement Regarding the Division of Corporation Finance's Role in the Exchange Act Rule 14a-8 Process for the Current Proxy Season issued by the Staff on November 17, 2025, we hereby request that the Staff confirm that it will not object if the Company omits the Proposal from the 2026 Proxy Materials. In this regard, the Company represents that it has a reasonable basis to exclude the Proposal based on the provisions of Rule 14a-8, prior published guidance, and/or judicial decisions.

As discussed in greater detail below, the Proposal may be excluded from the 2026 Proxy Materials pursuant to Rule 14a-8(i)(12)(iii) because the Proposal addresses substantially the same subject matter and substantive concerns—whether customers' use of the Company's products and services employing certain technologies contributes to human rights or similar violations—as shareholder proposals previously submitted by the Lead Proponent and others that were included in the Company's 2024, 2023, and 2022 proxy materials, and the most recent of those proposals did not receive the support necessary for resubmission under Rule 14a-8(i)(12)(iii).

A copy of the Proposal is attached to this letter as Exhibit A and incorporated herein by reference.

Pursuant to Rule 14a-8(j), we have:

- filed this letter with the Securities and Exchange Commission (the "Commission") no later than eighty (80) calendar days before the Company intends to file its definitive 2026 Proxy Materials with the Commission; and

- concurrently sent copies of this correspondence to the Proponents.

Rule 14a-8(k) and Staff Legal Bulletin No. 14D (Nov. 7, 2008) ("SLB 14D") provide that shareholder proponents are required to send companies a copy of any correspondence that the proponents elect to submit to the Commission or the Staff. Accordingly, we are taking this opportunity to inform the Proponents that if the Proponents elect to submit additional correspondence to the Commission or the Staff with respect to the Proposal, a copy of such correspondence should be furnished concurrently to the undersigned on behalf of the Company pursuant to Rule 14a-8(k) and SLB 14D.

THE PROPOSAL

The Proposal states:

> **Resolved**: Shareholders request the Board of Directors conduct an evaluation and issue a public report, at reasonable cost and omitting proprietary information, describing the alignment of Amazon's sale and deployment of artificial intelligence (AI) and related cloud technologies with its Responsible AI Approach. At the Board's discretion, the report should list and explain instances of misalignment, and state whether and how the identified incongruencies have or will be addressed.

ANALYSIS

The Proposal May Be Excluded Under Rule 14a-8(i)(12)(iii) Because The Proposal Addresses Substantially The Same Subject Matter As At Least Three Previous Proposals Included In The Company's Proxy Materials, And The Most Recent Of Those Proposals Did Not Receive The Support Necessary For Resubmission.

Under Rule 14a-8(i)(12)(iii), a shareholder proposal that "addresses substantially the same subject matter as a proposal, or proposals, previously included in the company's proxy materials within the preceding five calendar years" may be excluded from the proxy materials "if the most recent vote occurred within the preceding three calendar years and the most recent vote was . . . [l]ess than 25 percent of the votes cast if previously voted on three or more times."

A. Background On Rule 14a-8(i)(12).

The Commission has indicated that the condition in Rule 14a-8(i)(12) that the shareholder proposals deal with or address "substantially the same subject matter" does not mean that the previous proposal(s) and the current proposal must be exactly the same. Although the predecessor to Rule 14a-8(i)(12) required a proposal to be "substantially the same proposal" as previous proposals, the Commission amended this rule in 1983 to permit exclusion of a proposal that "deals with substantially the same subject matter." The Commission explained that this revision responded to commenters who viewed it as:

> [A]n appropriate response to counter the abuse of the security holder proposal process by certain proponents who make minor changes in proposals each year so that they can keep raising the same issue despite the fact that other shareholders have indicated by their votes that they are not interested in that issue.

Exchange Act Release No. 20091 (Aug. 16, 1983) (the "1983 Release"). *See also* Exchange Act Release No. 19135 (Oct. 14, 1982), in which the Commission stated that Rule 14a-8 "was not designed to burden the proxy solicitation process by requiring the inclusion of such proposals." In the release adopting this change, the Commission explained the application of the standard, stating:

> The Commission believes that this change is necessary to signal a clean break from the strict interpretive position applied to the [then-]existing provision. The Commission is aware that the interpretation of the new provision will continue to involve difficult subjective judgments, but anticipates that those judgments will be based upon a consideration of the substantive concerns raised by a proposal rather than the specific language or actions proposed to deal with those concerns.

B. Well-Established Precedents Demonstrate That A Proposal May Be Excluded Under Rule 14a-8(i)(12) When It Shares The Same Substantive Concerns As Previous Proposals Even If The Resolved Clause Differs In Scope From The Previous Proposals.

Consistent with the Commission's statement in the 1983 Release that the applicability of Rule 14a-8(i)(12) is "based upon a consideration of the substantive concerns raised by a proposal rather than the specific language or actions proposed to deal with those concerns," the Staff has concurred with exclusion of a proposal under Rule 14a-8(i)(12) when it addresses the same "substantive concerns" as previously voted on proposals, even when a subsequently submitted proposal differs in scope from the previous proposals. For example, in *Mondelēz International, Inc. (National Legal and Policy Center)* (avail. Mar. 25, 2025), the Staff concurred with exclusion under Rule 14a-8(i)(12) of a proposal requesting a report from the board's Governance, Membership and Sustainability Committee on the impact of the company's policy positions, advocacy, and charitable giving on social and political matters, and the effect of such actions on the company's financial stability. The company successfully argued that the proposal dealt with substantially the same subject matter as a previous proposal requesting the board

create a subcommittee of the audit committee to examine the risks and consequences of the company's associations with external organizations to determine whether such associations threaten the growth and sustainability of the company, noting that both proposals "address[ed] the same substantive concern—namely, the potential financial risk to the [c]ompany that may result from the [c]ompany's positions on social and political issues." Similarly, in *Exxon Mobil Corp. (Hild)* (avail. Mar. 20, 2024), the Staff concurred with exclusion under Rule 14a-8(i)(12) of a proposal requesting a report of the incurred costs and benefits "accrued to shareholders" from the company's activities related to its "ambition for net zero greenhouse gas emissions by 2050" that are voluntary because it addressed substantially the same subject matter as two previous proposals requesting a report on the costs and benefits "accrued to shareholders, the public health and the environment, including the global climate, from the company's environment-related activities that are voluntary." *See also Apple Inc.* (avail. Nov. 20, 2018) (concurring with the exclusion of a proposal requesting that the company review its policies related to human rights to assess whether it needed to adopt and implement additional policies because it dealt with substantially the same subject matter as a previous proposal requesting that the company establish a board committee on human rights and a second previous proposal requesting that the board amend the company's bylaws to require a board committee on human rights, noting that "[e]ach of the proposals specifically requests a review of the [c]ompany's practices and policies relating to human rights").

C. Consistent With The Foregoing Precedents, The Proposal May Be Excluded Because It Addresses Substantially The Same Substantive Concerns As Previous Proposals, And The Most Recent Proposal Failed To Gain Sufficient Shareholder Support.

The Proposal addresses substantially the same substantive concerns—whether customers' use of the Company's products and services employing certain technologies contributes to human rights or similar violations—as shareholder proposals submitted by the Lead Proponent and included in the Company's proxy materials for its 2024, 2023, and 2022 annual meetings of shareholders:

- The proposal in the Company's 2024 proxy materials (the "2024 Proposal") is attached to this letter as Exhibit B;
- The proposal in the Company's 2023 proxy materials (the "2023 Proposal") is attached to this letter as Exhibit C; and
- The proposal in the Company's 2022 proxy materials (the "2022 Proposal") is attached to this letter as Exhibit D.

The 2024 Proposal, the 2023 Proposal, and the 2022 Proposal are referred to collectively herein as the "Previous Proposals," and together with the Proposal, the "Proposals."

As evidenced in the Company's Form 8-K filed on May 24, 2024, which reports the voting results for the Company's 2024 Annual Meeting of Shareholders (and is attached to this letter

as Exhibit E), the 2024 Proposal received support from only 16.8% of the votes cast at the Company's 2024 Annual Meeting of Shareholders, well below the 25% threshold required for resubmission under Rule 14a-8(i)(12)(iii).[1]

Just as in the precedents discussed above, even though the "Resolved" clause of the Proposal differs from the resolved clause of the Previous Proposals, the Proposals address substantially the same subject matter. For example, the resolved clause of the Previous Proposals refers broadly to "products and services with surveillance, computer vision, or cloud storage capabilities," while the Proposal refers equally broadly to the "sale and deployment of artificial intelligence (AI) and related cloud technologies." Likewise, the Proposal shares the same substantive concerns regarding potential human rights violations, although it references those concerns differently. Specifically, while the Previous Proposals refer to assessing whether certain of the Company's products and services contributed to human rights violations, the Resolved clause of the Proposal refers to assessing whether certain products and services violate the Company's Responsible AI Approach but then the Proposal specifically highlights four aspects of the Company's Responsible AI Approach (fairness, privacy and security, safety, and transparency) that align with articles of the United Nations Universal Declaration of Human Rights.[2]

Moreover, the Proposals' supporting statements demonstrate that the Proposal raises the same substantive concerns and addresses substantially the same subject matter as the Previous Proposals that the Lead Proponent submitted to the Company, as reflected in the following chart.

Proposal	**2024 Proposal**	**2023 Proposal**	**2022 Proposal**
Each of the Proposals focuses on whether customers' use of Company products and services employing AI and cloud technologies contributes to human rights or similar violations			
"Amazon **continues to sell to and maintain contracts with entities engaged in rights-violating applications of its AI and related**	"Amazon Web Services (AWS) **serves multiple governmental customers with a history of human rights abuses. This raises the risk of**	"Amazon Web Services (AWS) **serves multiple governmental customers with a history of human rights abuses**, and Amazon's technologies	"Amazon Web Services (AWS) is a leading cloud provider that **serves multiple government customers with a history of human**

[1] The 2024 Proposal received 6,184,374,303 "against" votes and 1,248,281,806 "for" votes. Abstentions and broker non-votes were not included for purposes of this calculation. The total shareholder votes cast is calculated using a fraction for which the numerator is "for" votes and the denominator is "for + against" votes. See Staff Legal Bulletin No. 14, part F.4 (July 13, 2001).

[2] *Available at* https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Proposal	2024 Proposal	2023 Proposal	2022 Proposal
technologies, suggesting misalignment between policies and practice."	**product misuse by AWS customers** with poor human rights records, as Amazon's technologies may enable mass surveillance globally, as well as facilitate the targeting of human rights defenders, journalists, and political dissidents."	may enable mass surveillance globally."	**rights abuses**, and Amazon's surveillance technologies may enable mass surveillance globally."
Each of the Proposals raises concerns with use of certain Company products and services by the U.S. Department of Homeland Security and immigration enforcement			
"**AWS hosts many DHS databases and systems** used to track, monitor, and **deport immigrants**." "**AWS will host DHS' Homeland Advanced Recognition Technology (HART) system**, which will rely on AI to **store and process information about immigrants to facilitate detention and deportation**."	"**AWS will host the Department of Homeland Security's biometric database**, which will reportedly be used to '**assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation**.'"	"**AWS will host the Department of Homeland Security's biometric database**, which will reportedly be used to **'assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation**.'"	"**AWS will host the Department of Homeland Security's biometric database**, which will impact millions of immigrants' and citizens' 'ability to exercise their rights to protest, assemble, associate, and to live their daily lives.'" "**U.S. immigration enforcement agencies use AWS** in **detention and deportation programs**."
Each of the Proposals raises concerns with use of the Company's Ring products and services			
"**Amazon's Ring**, which produces doorbell cameras and	"**Amazon's Ring** continues to **infringe on citizens' privacy**,	"**Amazon's Ring** continues to **infringe on citizens' privacy**,	"Even after police used **Amazon's Ring** to surveil anti-racist

Proposal	2024 Proposal	2023 Proposal	2022 Proposal
has extensive partnerships with police departments, recently announced it will enable facial recognition, **drawing sharp criticism for creating new privacy and civil liberties risks**."	despite an audit and Ring's resulting changes. Its vague standards regarding **information sharing with law enforcement**, absent consent, led to **sharing of videos with law enforcement at least 11 times** in 2022. Ring continues to expand its **thousands of police partnerships**."	despite an audit and Ring's resulting changes. Its vague standards regarding **information sharing with law enforcement**, absent consent, led to **sharing of videos with law enforcement 11 times** in 2022. Ring continues to expand its **thousands of police partnerships**."	protesters and a UK court found **Ring infringed customer privacy, Ring continues to expand its thousands of police partnerships**."
Each of the Proposals raises concerns with use of the Company's products and services by the Israeli government			
"Its $1.2 billion **cloud computing contract with Israel - Project Nimbus** - has been used by Israel in its attacks on Palestinians . . . ."	"The **Israeli government's 'Project Nimbus,'** protested by Amazon employees, **uses AWS** to support the apartheid system . . . ."	"The **Israeli government's 'Project Nimbus,'** protested by Amazon employees, **uses AWS** to support the apartheid system . . . ."	"The **Israeli military and government's 'Project Nimbus'**, protested by Amazon employees, **uses AWS** to support and expand the apartheid system . . . ."
Each of the Proposals raises concerns with whether the Company's products and services employing AI and cloud technologies are sufficiently aligned with the Company's existing policies and commitments			
"Moreover, **because of the lack of transparency** about the specific ways Amazon's AI and related technologies are being used, **investors cannot be assured there is**	"Amazon's **existing policies appear insufficient in preventing customer misuse** and establishing effective oversight, yet Amazon continues releasing surveillance products.	"Amazon's **existing policies appear insufficient in preventing customer misuse** and establishing effective oversight, yet Amazon continues releasing surveillance products."	"Amazon's **existing policies appear insufficient in preventing customer misuse** and establishing effective oversight, yet Amazon continues releasing surveillance products."

Proposal	2024 Proposal	2023 Proposal	2022 Proposal
alignment with its commitments."	Moreover, **the company's disclosures make no mention of customer due diligence**, nor is there any relevant information about the process on its website."		
Each of the Proposals asserts that the Company's contracts with entities that the Proponents allege are engaged in "rights-violating applications" of the Company's products and services employing AI and cloud technologies present legal, regulatory, and reputational risks			
"Amazon **continues to sell to and maintain contracts with entities engaged in rights-violating applications of its AI and related technologies**, suggesting misalignment between policies and practice. Such misalignment **presents material legal, reputational, regulatory, and litigation risks** to Amazon and its investors."	"Inadequate customer due diligence **presents** material privacy and data security risks, as well as **legal, regulatory, and reputational risks** . . . ."	"Inadequate due diligence **presents** material privacy and data security risks, as well as **legal, regulatory, and reputational risks**."	"Inadequate due diligence **presents** material privacy and data security risks, as well as **legal, regulatory, and reputational risks**."

As demonstrated above, the Proposal shares the same substantive concerns and addresses substantially the same subject matter as the Previous Proposals. Each of the Proposals focuses on alleged human rights risks related to potential misuse of certain Company products and services, references the same examples to illustrate these concerns, raises concerns as to whether the Company's products and services are sufficiently aligned with its policies and commitments, and asserts that the situation presents legal, regulatory, and reputational risks. Although the resolved clause and scope of the Proposals differ, as was the case with the proposals in *Mondelēz International*, *Exxon Mobil*, and *Apple*, the differences do not change the

fact that the Proposal addresses substantially the same subject matter and shares the same substantive concerns as each of the Previous Proposals, and therefore does not preclude exclusion pursuant to Rule 14a-8(i)(12). Since the Company's shareholders have already voted on proposals addressing substantially the same subject matter as the Proposal in three previous years, and when most recently voted on the 2024 Proposal received support from only 16.8% of the votes cast, the Company may exclude the Proposal from its 2026 Proxy Materials under Rule 14a-8(i)(12)(iii).

CONCLUSION

We are available to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to shareholderproposals@gibsondunn.com. If we can be of any further assistance in this matter, please do not hesitate to call me at (202) 955-8671, or Susan Jong, the Company's Vice President, Associate General Counsel, and Corporate Secretary, at (206) 266-1000.

Sincerely,

Ronald O. Mueller

Enclosures

cc: Susan Jong, Amazon.com, Inc.
Aaron Acosta, Investor Advocates for Social Justice
Gina Haas, American Baptist Home Mission Society
Deborah Sagner
Sophie Lieberman
Amina Elfiki
coordinator@rjicoalition.org
ocaclientservices@obran.coop
Eliana Fishman
Rachel Lieberman
Catherine Rowan, Maryknoll Sisters of St. Dominic, Inc.
Pierluigi Ventura, PFC S.p.A. Società Benefit
Ann Scholz, School Sisters of Notre Dame Collective Investment Fund
Kate Schwartz
Dr. Omer A. Chaudhary
Sister Jean Anne Panisko, Sisters of Charity of Leavenworth
Julie N.W. Goodridge, NorthStar Asset Management, Inc.
Janis Cellini, Claudia Maria Cellini Argosy Trust UAD 12/24/93
Jody Leader
Marcela Pinilla, Zevin Asset Management

Barbara McCracken, Benedictine Sisters of Mount St. Scholastica
Séamus P. Finn, Missionary Oblates of Mary Immaculate-US Province
Bianca Agustin, United for Respect
Marcelline Koch, Dominican Sisters of Springfield, IL
Bernard Voyer, Durocher Fund
Sophia Vassilakidis
Dr. Nosheen Ahmad
Mathieu Robitaille
Katie Carter, PCUSA
Erin Ripperger, Portico Benefit Services
Ethan Birchard, Friends Fiduciary Corporation
Margaret C. Hughes
Nancy Murphy, The Daughters of Charity, Inc.
Lydia Kuykendal, Mercy Investment Services, Inc.
Frances Nadolny, Adrian Dominican Sisters
Jon Norstog

EXHIBIT A

Alignment Report

Resolved: Shareholders request the Board of Directors conduct an evaluation and issue a public report, at reasonable cost and omitting proprietary information, describing the alignment of Amazon's sale and deployment of artificial intelligence (AI) and related cloud technologies with its Responsible AI Approach. At the Board's discretion, the report should list and explain instances of misalignment, and state whether and how the identified incongruencies have or will be addressed.

Whereas: Amazon's Responsible AI Approach is guided by eight priorities, which include "fairness" (evaluating AI's impacts on different groups), "privacy and security" (appropriately obtaining and using data), "safety" (preventing harmful system output and misuse), and "transparency" (enabling stakeholders to make informed decisions about their engagement with AI).[1]

Despite this approach, Amazon continues to sell to and maintain contracts with entities engaged in rights-violating applications of its AI and related technologies, suggesting misalignment between policies and practice. Such misalignment presents material legal, reputational, regulatory, and litigation risks to Amazon and its investors.

For example, Amazon's cloud, AWS, is the world's most broadly adopted cloud and provides cloud computing, artificial intelligence, and data storage.[2] Its $1.2 billion cloud computing contract with Israel - Project Nimbus - has been used by Israel in its attacks on Palestinians, actions prominent organizations have classified as genocide.[3] Although the contract's details are not publicly available, a 2024 investigation found Israel had used AWS to store masses of military and surveillance data, and in some cases, to aid in airstrikes that killed many civilians.[4] An October 2025 investigation revealed the contract prohibits AWS from suspending, withdrawing, or restricting use of its technologies - even if Israel breaches AWS' terms of service - and requires AWS to violate court-imposed gag orders.[5]

Amazon's AI and related technologies also enable the US' expansive immigration crackdown, in which US Department of Homeland Security (DHS) agencies have been accused of arbitrary detentions, silencing free speech, and violating rights to privacy, nondiscrimination, asylum protections, due process, and other human rights.[6] AWS hosts many DHS databases and systems used to track, monitor, and deport immigrants.[7] AWS will host DHS' Homeland Advanced Recognition Technology (HART) system, which will rely on AI to store and process information about immigrants to facilitate detention and deportation.[8]

---

[1] https://www.aboutamazon.com/what-we-do/artificial-intelligence-ai/responsible-ai
[2] https://aws.amazon.com/what-is-aws/?nc1=f_cc
[3] https://www.un.org/unispal/wp-content/uploads/2025/09/a-hrc-60-crp-3.pdf
[4] https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/
[5] https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code
[6] https://rfkhumanrights.org/wp-content/uploads/2025/04/FINAL-UPR-Imm.-Coalition-Submission_4.7.25.pdf; https://www.youtube.com/watch?v=5zJpvgzxnwg&t=6s
[7] https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf
[8] https://surveillanceresistancelab.org/wp-content/uploads/2023/01/HART-Attack-2022.pdf

Amazon's Ring, which produces doorbell cameras and has extensive partnerships with police departments,[9] recently announced it will enable facial recognition,[10] drawing sharp criticism for creating new privacy and civil liberties risks.[11] Additionally, Ring announced a partnership with Flock, a network of AI-powered cameras whose data has been utilized by US Immigration and Customs Enforcement (ICE) in its immigration enforcement,[12] further increasing the risk that Amazon's AI will be misused to violate human rights.

Moreover, because of the lack of transparency about the specific ways Amazon's AI and related technologies are being used, investors cannot be assured there is alignment with its commitments.

[9] https://www.wbur.org/hereandnow/2025/09/30/ring-police-partnerships
[10] https://www.washingtonpost.com/technology/2025/10/03/amazon-ring-doorbell-facial-recognition-pricacy/
[11] https://www.markey.senate.gov/news/press-releases/senator-markey-demands-amazon-abandon-plan-to-include-facial-recognition-technology-in-ring-doorbells
[12] https://techcrunch.com/2025/10/16/amazons-ring-to-partner-with-flock-a-network-of-ai-cameras-used-by-ice-feds-and-police/; https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/; https://www.aclu.org/news/privacy-technology/flock-massachusetts-and-updates

EXHIBIT B

ITEM 6—SHAREHOLDER PROPOSAL REQUESTING A REPORT ON CUSTOMER DUE DILIGENCE

Beginning of Shareholder Proposal and Statement of Support:

Customer Due Diligence

Resolved: Shareholders request the Board of Directors commission an independent third-party report, at reasonable cost and omitting proprietary information, assessing Amazon's customer due diligence process to determine whether customers' use of its products and services with surveillance, computer vision, or cloud storage capabilities contributes to human rights violations or violates international humanitarian law.

Whereas: Amazon Web Services (AWS) serves multiple governmental customers with a history of human rights abuses. This raises the risk of product misuse by AWS customers with poor human rights records, as Amazon's technologies may enable mass surveillance globally, as well as facilitate the targeting of human rights defenders, journalists, and political dissidents.

Since the universal endorsement of the United Nations Guiding Principles for Business and Human Rights in 2011,[1] conducting human rights due diligence (HRDD) has become the de-facto standard in the tech sector.[2] Conducting HRDD, which includes customer risk assessments, mitigates clients' risks and human rights impacts and informs business decision-making by helping to identify the likelihood of technology misuse to facilitate governmental human or civil rights violations.[3] Furthermore, the Atlantic Council has recommended the US create know-your-customer policies with surveillance companies.[4]

Inadequate customer due diligence presents material privacy and data security risks, as well as legal, regulatory, and reputational risks, which are particularly pertinent when considering the sale and use of sensitive and emerging technologies. Amazon's product portfolio contains several products with potentially grave misuse capabilities. Despite Amazon's indefinite moratorium of its Rekognition face comparison feature, it has not clarified how Rekognition is still used by police outside of "criminal investigations."[5] Additionally, Amazon's Ring continues to infringe on citizens' privacy, despite an audit and Ring's resulting changes.[5] Its vague standards regarding information sharing with law enforcement, absent consent, led to sharing of videos with law enforcement at least 11 times in 2022.[6] Ring continues to expand its thousands of police partnerships.[6]

At the same time, Amazon's government-affiliated customers with a history of rights-violating behavior pose risks to the company, including:

- AWS will host the Department of Homeland Security's biometric database, which will reportedly be used to "assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation";[7]
- The Israeli government's "Project Nimbus," protested by Amazon employees,[8] uses AWS to support the apartheid system under which Palestinians are surveilled, unlawfully detained, and tortured.[9] Israel plans to use AWS as it expands illegal settlements and enforces segregation. The UN has clearly indicated war crimes may have been committed by Amazon's major customer, the Israel Defense Forces, since October 7, 2023.[10]

Amazon's existing policies appear insufficient in preventing customer misuse and establishing effective oversight, yet Amazon continues releasing surveillance products. Moreover, the company's disclosures make no mention of customer due diligence, nor is there any relevant information about the process on its website.

---

1 https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

2 https://www.humanrights.dk/sites/humanrights.dk/files/media/document/Phase%204_%20Impact%20prevention%20mitigation%20and%20remediation_ENG_accessible.pdf

3 https://www.humanrights.dk/sites/humanrights.dk/files/media/document/Phase%204_%20Impact%20prevention%20mitigation%20and%20rediation_ENG_accessible.pdf; https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic

4 https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf

5 https://s2.q4cdn.com/299287126/files/doc_financials/2022/ar/Amazon-2022-Proxy-Statement.pdf

6 https://www.markey.senate.gov/imo/media/doc/amazon_response_to_senator_markey-july_13_2022.pdf

[7] https://www.immigrantdefenseproject.org/wp-content/uploads/HART-Attack.pdf

[8] https://www.forbes.com/sites/richardnieva/2022/09/09/google-and-amazon-protest-project-nimbus-ai-contract-israel/?sh=68609827d162

[9] https://www.hrw.org/news/2021/11/24/mass-surveillance-fuels-oppression-uyghurs-and-palestinians; https://www.amnesty.org/en/documents/mde15/5141/2022/en/; https://www.gov.il/en/departments/news/press_01082023_b

[10] https://www.ohchr.org/en/press-releases/2023/10/commission-inquiry-collecting-evidence-war-crimes-committed-all-sides-israel

End of Shareholder Proposal and Statement of Support

Shareholder: American Baptist Home Mission Society

RECOMMENDATION OF THE BOARD OF DIRECTORS ON ITEM 6

Why We Recommend You Vote Against This Proposal

- We are committed to the responsible use of our artificial intelligence and machine learning (AI/ML) products and services and other AWS services and believe these products and services promote safety and security and significantly benefit society.
- For the fifth year in a row, this proposal continues to rely on the same speculative and outdated concerns and mischaracterizations and fails to take into account the fact that:
  - Over the seven years that AWS has been offering Amazon Rekognition and the six years since we acquired Ring, we have been updating our technology and enhancing safeguards and have avoided or mitigated the risks and concerns posited in this proposal;
  - AWS has never received a single verified report of Amazon Rekognition being used in the harmful manner posited in the proposal; and
  - Our Nominating and Corporate Governance Committee has specifically reviewed Amazon Rekognition's facial recognition capabilities and Ring, focusing on the actual operation and use of Amazon Rekognition and Ring, the potential concerns and misuse that could arise from these technologies, and our actions to resolve or mitigate those risks and concerns.
- We have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, product development processes, customer contractual requirements and training, consultation with third party experts, and other policies and practices. For example:
  - Credo AI, a company that specializes in responsible AI, has performed a third-party evaluation, which supports that Rekognition performs well across demographic attributes.
  - In 2020, we implemented a global moratorium on police use of Amazon Rekognition's facial comparison feature in connection with criminal investigations.
  - As part of an ongoing commitment to improving its products and services by soliciting feedback from community stakeholders and independent experts, Ring completed a civil rights and civil liberties audit with the Policing Project at New York University School of Law in 2021, during the course of which Ring implemented over one hundred changes to its products, policies, and legal processes.
  - Also, as part of a number of changes Ring recently made to the Neighbors app, Ring sunset the Request for Assistance tool. While public safety agencies can still share important updates and ask for help from their communities, they can no longer use the Request for Assistance tool to receive videos through the app.

Amazon's Technology Products and Services Have the Demonstrated Capability to Solve Complex Problems and Benefit Society

We believe strongly in harnessing the capabilities of advanced technology such as the cloud, artificial intelligence, and machine learning to: promote the ongoing safety and security of our fellow citizens, our communities, and the world; solve complex problems; and benefit society. While we understand the concerns over potential misuse, we believe these are effectively addressed through the policies and procedures we have adopted and that we continue to advance with input from internal and third-party partners and stakeholders.

When used properly and responsibly, the technology products and services offered by Amazon provide substantial benefits to society and the communities and organizations that use them. For example, since being introduced in 2016, non-profit, advocacy, and government groups have used Amazon Rekognition's facial recognition capabilities to protect human rights, including tracking and stopping child exploitation and rescuing victims of human trafficking, as well as locating hundreds of missing children.[10] Similarly, Ring continues to innovate by inventing home security products that solve real customer problems and assisting community members in sharing important community information and connecting with each other. These are just a few of the numerous beneficial applications of these technologies.

The proposal requests that the Company prepare a report about Amazon's process for customer due diligence to determine whether customers' use of certain of our products or services contributes to human rights violations or violates international humanitarian law. Conversations around responsible development and use of AI/ML systems are happening around the world among government, industry, academia, and other groups. Amazon is an active participant and contributor to these conversations, and Amazon teams and subject matter experts are helping lead the industry on these very issues. As discussed below, we have conscientiously acted to review and address the concerns expressed in the proposal and transparently provided information regarding our actions to the public.

This Proposal Fails to Acknowledge or Address the Numerous Measures We and Our Board of Directors Have Taken to Address the Proposal's Concerns Over the Course of Years and Instead Relies on Speculative and Outdated Claims and Mischaracterizations

While we have been working to constantly enhance our AI/ML technology, including for Amazon Rekognition and Ring products and services, and have avoided or mitigated the risks and concerns posited in this proposal, for the fifth year in a row this proposal continues to rely on the same outdated assertions and mischaracterizations. For example, this proposal continues to incorrectly insinuate that Amazon Rekognition is a surveillance program. In fact, Amazon Rekognition does not collect images for users to perform searches on and does not provide any photos or data for users to search or compare images against. Instead, the service can be used to help analyze or detect objects, people, text, scenes, and activities in images and videos, as well as to detect inappropriate content, fraudulent users, or bots. In addition, AWS provides a website and e-mail address where any person can report suspected abuse, and AWS employs trained staff that review every report that is received. In the more than seven years AWS has been offering Amazon Rekognition, AWS has never received a single verified report of Amazon Rekognition being used in the harmful manner posited in the proposal. Further, this proposal does not take into account the Policing Project's civil rights and civil liberties audit and the review and feedback Ring received from the Center for Democracy and Technology (the "CDT"), and instead uses vague innuendo, outdated claims, and mischaracterizations to suggest concerns with the operation of our policies and our products. We believe our actions demonstrate that we are willing to work constructively to address realistic issues and work toward solutions that continue to allow customers to benefit from useful technologies, while the proposal and its supporting statements year after year repeat their generalized concerns and dismiss our numerous actions to proactively assess and mitigate risks.

Our Board has reviewed Amazon Rekognition, along with many other programs, as part of numerous AWS business reviews, and has also reviewed Ring over the course of several meetings since our acquisition of Ring. In addition, our Nominating and Corporate Governance Committee provides oversight on behalf of the Board over the human rights aspects of Amazon's Rekognition technology and Ring, as well as our other technologies, and has specifically reviewed Amazon Rekognition's facial recognition capabilities and Ring. These reviews focus on the actual operation and use of Amazon Rekognition and Ring, the potential concerns and misuse that could arise from these technologies, and our actions to resolve or mitigate those risks and concerns. Under its charter, the Nominating and Corporate Governance Committee, which is comprised of directors with experience in emerging technologies and public policy, is responsible for overseeing and monitoring the Company's policies and initiatives relating to corporate social responsibility, including human rights and ethical business practices, and risks related to the Company's operations and engagement with customers, suppliers, and communities.

We Are Committed to the Responsible Use of Our AI/ML Products and Services and Other AWS Services, and the Proponents Have Failed to Acknowledge or Address the Numerous Actions We Have Taken to Address Concerns Around Potential Misuse of Rekognition and Ring Products

Since introducing Amazon Rekognition, we have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, product development processes, customer contractual requirements and training, consultation with third party experts, and other policies and practices. We understand the risks

[10] See *https://www.aboutamazon.com/news/innovation-at-amazon/how-amazon-rekognition-helps-in-the-fight-against-some-of-the-worst-types-of-crime*.

associated with potential misuse of facial recognition technology and, in connection with extensive discussions with customers, researchers, academics, policymakers, and civil society groups, we have taken the following actions to address concerns around potential misuse:

- *Implemented Police Moratorium.* In June 2020, AWS implemented a global moratorium on use of Amazon Rekognition's face comparison feature by police departments in connection with criminal investigations and, in May 2021, AWS announced the indefinite extension of that moratorium. In addition to our implementation of the moratorium on police use and legal terms for law enforcement use, AWS continues to engage with a large number of diverse stakeholders on these issues, including civil society groups, academia, policymakers, and law enforcement officials. As discussed below, we support appropriate legislative or regulatory frameworks to protect individual civil rights and ensure that governments are transparent in their use of facial recognition technology, and have consulted with and provided support to those working to address these issues.[11]
- *Provide Customers with Responsible AI and Transparency Tools.* Our commitment to developing AI and ML in a responsible way is integral to how we build our services, engage with customers, and drive innovation. We are committed to providing customers with tools and resources to develop and use AI/ML responsibly. For example, in November 2022, we launched AWS AI Service Cards, a transparency resource to help customers better understand our AWS AI services. AWS has published several detailed AI Service Cards, including cards for Rekognition Face Matching and Rekognition Face Liveness.[12] AI Service Cards are a form of responsible AI documentation that provides customers with a single place to find information on the intended use cases and limitations, responsible AI design choices, and deployment and performance optimization best practices for an AI service or feature. They are part of our evolving comprehensive development process we undertake to build our services in a responsible way that addresses fairness and bias, explainability, robustness, governance, transparency, privacy, and security in a state-of-the-art manner. AI Service Cards will continue to evolve and expand as we engage with our customers and the broader community to gather feedback and continually iterate on our approach.
- *Dedicate Significant Resources to AI/ML Accuracy and Bias Mitigation.* AWS dedicates significant resources to testing and developing its technology to constantly improve accuracy and performance. AWS also focuses on promoting diverse perspectives on its technology development teams, using diverse training and evaluation data sets (e.g., representative across demographic groups), and incorporating feedback from third parties. For example, Credo AI, a company that specializes in Responsible AI, has performed a third-party evaluation of Rekognition using an identity verification data set containing high-quality images of subjects with good lighting, no blur, and no occlusion. The evaluation supports our finding that Rekognition performs well across demographic attributes.[13] We have science and technical experts who help promote fairness in our products and services, including helping to design, test, and assess our services for fairness and accuracy and to mitigate potential bias, and who publish academic papers and provide thought leadership in this area.[14] We also offer tools and resources to customers, such as Amazon SageMaker Clarify, which helps customers detect and mitigate potential bias in ML models and data using a variety of metrics and helps explain model predictions.[15] We continue to invest heavily in this area and work closely with customers and other stakeholders on addressing these important issues.
- *Actively Engage in Policy Discussions.* Amazon believes that facial recognition technology should not be banned or condemned simply because there is a potential that people may misuse it. Many technologies, like cell phones or cameras, could also be misused. Instead, as we have made clear in our statement of positions, "we think that governments and lawmakers should act to regulate the use of this technology to ensure it's used appropriately, and we have proposed guidelines for effective regulatory frameworks and guardrails that protect individual civil rights and ensures that governments are transparent in their application of the technology."[16] In July 2023, we joined President Biden and leaders across government and industry to voluntarily commit to continue promoting the safe, secure, and transparent development of AI technology that benefits society.[17] We also participated in the UK AI Safety Summit where we built upon the White House Voluntary AI Commitments by sharing relevant aspects of our responsible AI development practices

---

11 Available at *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

12 See *https://aws.amazon.com/machine-learning/responsible-ai/resources/*.

13 See *https://aws.amazon.com/machine-learning/responsible-machine-learning/rekognition-face-matching/*.

14 Available at *https://arxiv.org/abs/2007.06570* (submitted Jul. 13, 2020), and *https://www.youtube.com/watch?v=JCGUYFe6P2k*. See also *https://www.amazon.science/blog/method-predicts-bias-in-face-recognition-models-using-unlabeled-data* (Nov. 8, 2022).

15 Available at *https://aws.amazon.com/sagemaker/clarify/*.

16 Available at *https://www.aboutamazon.com/about-us/our-positions* and *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

17 See *https://www.aboutamazon.com/news/company-news/amazon-responsible-ai/*.

and protocols with the global community.[18] In addition, we announced that we have joined the U.S. Artificial Intelligence Safety Institute Consortium, established by the National Institute of Standards and Technology ("NIST"), as part of our efforts to further government and industry collaboration to advance safe and secure AI.[19]

- *Support Standardized Testing Methodologies and Benchmarks.* We believe it is important that there be standardized testing methodologies and benchmarks for cloud-based facial recognition technologies. AWS encourages and supports the development of independent standards by entities like NIST and other independent and recognized research organizations and standards bodies to develop tests, including those that support cloud-based facial recognition software. We are engaging with NIST and other stakeholders to offer our direct assistance towards this effort. We also support efforts by members of the academic and commercial community to establish independent and trusted criteria, benchmarks, and evaluation protocols for AI/ML technology, including facial recognition services.
- *Partner and Collaborate with External Stakeholders.* AWS collaborates with the academic community and other stakeholders on the responsible use of AI/ML technologies. For example, through our participation in Partnership on AI, we have worked with leading technology companies and organizations such as the ACLU, Future of Privacy Forum, and the MIT Initiative on the Digital Economy to advance public understanding of AI technologies and address opportunities and challenges with AI technologies to benefit people and society, focusing on areas such as ethics, fairness, inclusivity, and transparency. We are also active participants in other multi-stakeholder organizations relating to AI, including The Organisation for Economic Co-operation and Development (OECD) working groups on AI, the Global Partnership on AI, and the Responsible AI Institute. We provide research grants through Amazon Research Awards and the joint Amazon and National Science Foundation Fairness in AI Grants program.
- *Require Customer Agreement to Acceptable Use Policy and Responsible AI Policy.* As a condition to using any AWS service, including Amazon Rekognition, a customer (including any government or law enforcement customer) must agree to the AWS Acceptable Use Policy (the "AUP"), which prohibits use of AWS's services "for any illegal or fraudulent activity."[20] This includes the violation of any laws related to privacy, discrimination, and civil rights. AWS will investigate and take appropriate action, including potentially removing or disabling access to Amazon Rekognition or any other AWS service if we determine a customer is violating our AUP or the AWS legal terms. We also recently published the AWS Responsible AI Policy to supplement the AUP, which applies to the use of all AWS AI/ML services.[21] The AWS Responsible AI Policy explicitly prohibits the use of AWS AI/ML services, features, and functionality we provide (1) for intentional disinformation or deception; (2) to violate the privacy rights of others, including unlawful tracking, monitoring, and identification; (3) to depict a person's voice or likeness without their consent or other appropriate rights, including unauthorized impersonation and non-consensual sexual imagery; (4) for harm or abuse of a minor, including grooming and child sexual exploitation; (5) to harass, harm, or encourage the harm of individuals or specific groups; (6) to intentionally circumvent safety filters and functionality or prompt models to act in a manner that violates our policies; or (7) to perform a lethal function in a weapon without human authorization or control. In addition, the AWS Responsible AI Policy provides that customers using AI/ML services to make consequential decisions impacting a person's fundamental rights, health, or safety must evaluate the potential risks of their use cases and implement appropriate human oversight, testing, and other use case-specific safeguards to mitigate such risks.
- *Enhanced Legal Terms.* All customers using any AWS service must comply with the relevant AWS legal terms. In early 2020, prior to our implementation of the moratorium on police use, we spent significant resources and consulted with law enforcement customers, civil society groups, and other stakeholders to perform an extensive review of and update to our legal terms to require certain disclosures and practices around certain law enforcement use cases. For example, if Amazon Rekognition is used to assist in identifying a person, and actions will be taken based on the identification that could impact that person's civil liberties or equivalent human rights, AWS legal terms require the decision to take action to be made by an appropriately trained person based on their independent examination of the identification evidence, and require the agency to ensure that such personnel receive appropriate training on the responsible use of facial recognition systems.[22] We believe this framework strikes a balance between the benefits and risks of use of facial recognition by law enforcement and helps address concerns around potential misuse.
- *Provide Customer Guidance on Best Practices and Responsible Use.* AWS provides guidance to customers on best practices for utilizing and analyzing the results from using facial recognition technology. For example, in line with the AWS legal

---

18 See *https://aws.amazon.com/uki/cloud-services/uk-gov-ai-safety-summit/*.

19 See *https://www.aboutamazon.com/news/policy-news-views/amazon-joins-us-artificial-intelligence-safety-institute-to-advance-responsible-ai*.

20 Available at *https://aws.amazon.com/aup/*.

21 Available at *https://aws.amazon.com/machine-learning/responsible-ai/policy*.

22 See *https://aws.amazon.com/service-terms/*.

terms described above, AWS recommends that in public safety use cases human reviewers verify the system's results and decisions not be made based on the system output without additional human review. AWS also recommends in these use cases that customers be transparent about the use of face detection and comparison systems including, wherever possible, informing end users and subjects about the use of these systems, obtaining consent for that use, and providing a mechanism for end users and subjects to provide feedback to improve the system.[23] AWS also provides publicly available guidance to customers and other interested parties on the responsible design, deployment, and use of ML systems in its Responsible Use of Machine Learning Guide.[24] Further, customers can engage an AWS team of experts in responsible AI/ML to recommend and help apply existing use-case-specific best practices on the development, deployment, and operationalization of responsible ML principles.[25] When we are approached by or become aware of customers with potential use cases that may implicate our AUP or other terms, we analyze the proposed use case to determine whether it complies with these terms. We have turned down customers whose proposed uses would violate our AUP or other terms.

We have taken the following actions, among others, to limit potential misuse of Ring products and services:

- *Give Users Control and Innovate on Their Behalf.* The Neighbors App by Ring is a free application designed to help community members connect with each other and trusted sources of safety information like the public safety agencies that serve them. Ring designed Neighbors to protect user privacy and to keep users in control of what information, if any, they want to share. Users can choose whether or not to upload videos, photos, or text-based posts to Neighbors to publicly share information with their communities. In addition, as part of a number of changes Ring recently made to the Neighbors app, Ring sunset the Request for Assistance tool. While public safety agencies can still share important updates and ask for help from their communities, they can no longer use the Request for Assistance tool to receive videos through the app. Ring does not provide police and other public safety officials access to device livestreams or control of user devices.
- *Audit with the NYU Policing Project and Continued Commitment to External Feedback.* In 2021, Ring completed a civil rights and civil liberties audit with the Policing Project at New York University School of Law to help Ring promote equity, transparency, and accountability in its products and services. The audit entailed nearly two years of work and was focused on potential racial justice, civil rights, civil liberties, and democratic accountability issues relating to both law enforcement's use of Neighbors and Ring's practices regarding law enforcement requests for information, including emergency requests for information. Based on recommendations and observations developed during the course of the audit, Ring implemented over one hundred changes to its products, policies, and legal processes.[26] Changes such as adding community resources like mental health services to the Neighbors App, were cited by the Policing Project as steps Ring has taken to safeguard against improper use and address potential harms. Ring also actively solicits feedback on its products and services from independent experts, like the National Network to End Domestic Violence and the CDT, to maintain different perspectives at the forefront of Ring's work.
- *Require Customer Agreement to Community Guidelines.* Ring is committed to upholding a standard of trust and civility and does not tolerate racial profiling, hate speech, and other forms of profiling or prejudice on Neighbors. Ring requires all Neighbors users, including public safety and local government agencies, to agree to strict community guidelines, which prohibit racial profiling, hate speech, and other forms of discrimination. Ring has a dedicated group of team members, who are trained regarding critical and timely issues, proactively moderating Neighbors content and reviewing posts and comments before they are published. When posts are denied, an email is sent to the Neighbors user who submitted the post to inform them of the reason, reinforcing our guidelines and helping users make responsible decisions. In addition, Neighbors users can flag incorrect or inappropriate content directly in the App. The moderation team will remove the flagged content if they determine that the content violates community guidelines. Ring also engaged the CDT to provide feedback and help strengthen Ring's moderation practices, and the CDT contributed to updates to the Neighbors App and community guidelines in 2021 and continues to provide feedback to Ring today.
- *Share Clear Law Enforcement Guidelines*. Like any other company, Ring is obligated to review and respond to legally binding requests for information from law enforcement. Ring does not disclose customer information to law enforcement in connection with government demands unless we are compelled to do so to comply with law (i.e., legally valid and binding requests for information from law enforcement agencies such as search warrants signed by a judge, subpoenas,

[23] Available at *https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf*.

[24] See *https://d1.awsstatic.com/responsible-machine-learning/responsible-use-of-machine-learning-guide.pdf*.

[25] See *https://pages.awscloud.com/GLOBAL-aware-IND-AWS-ProServe-Responsible-ML-2021-reg.html*.

[26] For more information on the Policing Project's civil rights and civil liberties audit, see *https://www.policingproject.org/ring*.

and court orders). Ring carefully reviews each of these requests and challenges those that we believe to be overbroad or otherwise inappropriate. As part of the NYU Policing Project audit, Ring updated its law enforcement information request reporting to share the type and number of binding information requests processed on a biannual basis.[27] Like many other companies, on rare occasions Ring may provide information to law enforcement on an emergency basis when there is an imminent danger of death or serious physical injury, such as a kidnapping or an attempted murder. Ring has robust policies and practices for evaluating these requests. Trained members of the legal team carefully review these submissions and emergency requests are regularly denied. These policies have long been reflected in Ring's public-facing Law Enforcement Guidelines.

- *Deliver on Privacy and Security Commitment.* Ring continues to innovate and identify new ways to help uphold customer privacy and security and give users even more control over their devices and personal information. For example, Ring launched video end-to-end encryption for non-battery powered cameras and doorbells in the United States in early 2021, a feature that allows customers to further secure their videos with an additional virtual lock, which can only be unlocked by a key that is stored on the customer's enrolled mobile device, designed so that only the customer can decrypt and view recordings on their enrolled device. In 2022, Ring expanded support for video end-to-end encryption to most of its battery-powered camera and doorbell devices, and to additional countries outside of the United States.

In light of our commitment to customer trust, privacy, and security; the substantial benefits to both society and organizations of Amazon's technology products and services; and our ongoing transparency and efforts to address potential misuse of those products and services, the Board recommends that shareholders vote against this proposal.

The Board of Directors recommends a vote "AGAINST" this proposal requesting a report on customer due diligence.

ITEM 7—SHAREHOLDER PROPOSAL REQUESTING ADDITIONAL REPORTING ON LOBBYING

Beginning of Shareholder Proposal and Statement of Support:

Resolved, shareholders of Amazon request the preparation of a report, updated annually, disclosing:

1. Company policy and procedures governing lobbying, both direct and indirect, and grassroots lobbying communications.

2. Payments by Amazon used for (a) direct or indirect lobbying or (b) grassroots lobbying communications, in each case including the amount of the payment and the recipient.

3. Description of management's and the Board's decision-making process and oversight for making payments described in sections 2 above.

For purposes of this proposal, a "grassroots lobbying communication" is a communication directed to the general public that (a) refers to specific legislation or regulation, (b) reflects a view on the legislation or regulation and (c) encourages the recipient of the communication to take action with respect to the legislation or regulation. "Indirect lobbying" is lobbying engaged in by a trade association or other organization of which Amazon is a member.

Both "direct and indirect lobbying" and "grassroots lobbying communications" include efforts at the local, state and federal levels.

The report shall be presented to the Audit Committee and posted on Amazon's website.

[27] See *https://ring.com/law-enforcement-information-requests*.

EXHIBIT C

We Are a Leader in Environmental Sustainability

We recognize that human-induced climate change is real and that action is needed from the public and private sectors, and, as observed by the proposal, we have taken actions to address climate change. Those actions include adopting ambitious operational climate goals and making significant progress in those areas. For example, with our co-founder Global Optimism, in 2019 we announced The Climate Pledge, a goal to reach net-zero carbon emissions across our operations by 2040, a decade ahead of the Paris Agreement's goal of 2050.[2] We are on a path to powering our operations with 100% renewable energy by 2025, five years ahead of our original target of 2030.[3]

In light of the fact that (i) the responsible plan fiduciary must select the 401(k) investment options, including the default investment option, in accordance with the requirements of U.S. federal law and (ii) our 401(k) plan offers a broad range of investment strategies, taking into account a variety of potential risks, reward opportunities, and goals, including, but not limited to, those related to climate change, the Board recommends shareholders vote against the proposal.

The Board of Directors recommends a vote "AGAINST" this proposal requesting a report on retirement plan options.

ITEM 7—SHAREHOLDER PROPOSAL REQUESTING A REPORT ON CUSTOMER DUE DILIGENCE

Beginning of Shareholder Proposal and Statement of Support:

Customer Due Diligence

Resolved: Shareholders request the Board of Directors commission an independent third-party report, at reasonable cost and omitting proprietary information, assessing Amazon's customer due diligence process to determine whether customers' use of its products and services with surveillance, computer vision, or cloud storage capabilities contributes to human rights violations.

Whereas: Amazon Web Services (AWS) serves multiple governmental customers with a history of human rights abuses, and Amazon's technologies may enable mass surveillance globally.

"Know Your Customer" due diligence mitigates clients' risks and human rights impacts and informs business decision-making.[1] It reveals whether technologies will be used to facilitate governmental human or civil rights violations.[2] The Atlantic Council recommended the United States (U.S.) "create know-your-customer policies" with surveillance companies.[3] The United Nations found states and businesses have "often rushed to incorporate AI applications, failing to carry out due diligence."[4]

Inadequate due diligence presents material privacy and data security risks, as well as legal, regulatory, and reputational risks. These risks are present even if surveillance products are used according to Amazon's guidelines. Despite Amazon's indefinite moratorium of its Rekognition face comparison feature, it has not clarified how Rekognition is still used by police outside of "criminal investigations."[5] Amazon's Ring continues to infringe on citizens' privacy, despite an audit and Ring's resulting changes. Its vague standards regarding information sharing with law enforcement, absent consent, led to sharing of videos with law enforcement 11 times in 2022. Ring continues to expand its thousands of police partnerships.[6] Civil rights groups have sharply criticized Amazon's MGM show, Ring Nation, calling it a "transparent attempt to normalize surveillance."[7]

Amazon's government-affiliated customers and suppliers with a history of rights-violating behavior pose risks to the company, including:

- AWS will host the Department of Homeland Security's biometric database, which will reportedly be used to "assemble target lists for ICE raids, expand the tech border wall, and to facilitate surveillance, arrests, immigrant detention and deportation";[8]

[2] See Amazon's 2021 Sustainability Report: Delivering Progress Every Day, at 10, available at *https://sustainability.aboutamazon.com/2021-sustainability-report.pdf*.

[3] *Id.* at 9.

- Amazon sells relabeled surveillance products in the U.S. from Chinese companies Dahua and Hikvision, which have been blacklisted by the U.S. Government and implicated in mass surveillance, internment, torture, and forced labor of the ethnic Uyghur minority;[9]
- The Israeli government's "Project Nimbus," protested by Amazon employees,[10] uses AWS to support the apartheid system under which Palestinians are surveilled, unlawfully detained and tortured.[11] Israel plans to use AWS as it expands illegal settlements and enforces segregation;
- AWS opened a data center in United Arab Emirates, a country that deploys a state surveillance apparatus targeting human rights defenders, journalists, and political dissidents[12]. AWS' first data center in the region opened in Bahrain, which has a poor human rights record.

Amazon's existing policies[13] appear insufficient in preventing customer misuse and establishing effective oversight, yet Amazon continues releasing surveillance products.

---

1 https://www.humanrights.dk/sites/humanrights.dk/files/media/document/Phase%204_%20Impact%20prevent

2 https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards- evaluating-domestic

3 https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf

4 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E

5 https://s2.q4cdn.com/299287126/files/doc_financials/2022/ar/Amazon-2022-Proxy-Statement.pdf

6 https://www.markey.senate.gov/imo/media/doc/amazon_response_to_senator_markey-july_13_2022.pdf

7 https://www.cancelringnation.com/

8 https://justfutureslaw.org/wp-content/uploads/2022/05/HART-Attack.pdf

9 https://ipvm.com/reports/amazon-powers-hikua

10 https://www.forbes.com/sites/richardnieva/2022/09/09/google-and-amazon-protest-project-nimbus-ai-contract-israel/?sh=68609827d162

11 https://www.hrw.org/news/2021/11/24/mass-surveillance-fuels-oppression-uyghurs-and-palestinians; https://www.amnesty.org/en/documents/mde15/5141/2022/en/

12 https://smex.org/amazon-launches-data-region-in-the-uae/

13 https://sustainability.aboutamazon.com/people/human-rights/principles; https://ir.aboutamazon.com/corporate-governance/documents-and-charters/code-of-business-conduct-and-ethics/default.aspx; https://aws.amazon.com/agreement/

End of Shareholder Proposal and Statement of Support

Shareholder: American Baptist Home Mission Society

RECOMMENDATION OF THE BOARD OF DIRECTORS ON ITEM 7

Why We Recommend You Vote Against This Proposal

- Amazon is committed to the responsible use of our artificial intelligence and machine learning (AI/ML) products and services and other AWS services. We have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, customer contractual requirements and training, consultation with third party experts, and other policies and practices.
- For example, Credo AI, a company that specializes in responsible AI, performed a third-party evaluation, which supports that Rekognition performs well across demographic attributes. In 2020, we implemented a global moratorium on police use of Amazon Rekognition's facial comparison feature for criminal investigations. As part of an ongoing commitment to improving its products and services by soliciting feedback from community stakeholders and independent experts, Ring completed a civil rights and civil liberties audit with the Policing Project at New York University School of Law in 2021, during the course of which Ring implemented over one hundred changes to its products, policies, and legal processes. Ring continues to engage with community stakeholders and independent experts like the Center for Democracy and Technology.
- Over the six years that AWS has been offering Amazon Rekognition and the five years since we acquired Ring, we have been updating our technology and enhancing safeguards and have avoided or mitigated the risks and concerns expressed in this proposal. For example, AWS has not received a single verified report of Amazon Rekognition being used in the harmful manner posited in the proposal.

Amazon's Technology Products and Services Have the Demonstrated Capability to Solve Complex Problems and Benefit Society

We believe strongly in harnessing the capabilities of advanced technology such as the cloud and machine learning to promote ongoing safety and security of our fellow citizens, our communities, and the world. While we understand the concerns over potential misuse, we believe these are effectively addressed through the policies and procedures we have adopted and that we continue to advance with input from internal and third-party partners and stakeholders.

When used properly and responsibly, the technology products and services offered by Amazon provide material benefits to society and the communities and organizations that use them. For example, since being introduced in 2016, non-profit, advocacy, and government groups have used Amazon Rekognition's facial recognition capabilities to protect human rights, including tracking and stopping child exploitation and rescuing victims of human trafficking, as well as locating hundreds of missing children.[4] Similarly, Ring strives to fulfill its mission to make neighborhoods safer, including by inventing home security products that solve real customer problems and assisting community members in sharing important safety information and connecting with each other. These are just a few of the numerous beneficial applications of these technologies.

We Are Committed to the Responsible Use of Our AI/ML Products and Services and Other AWS Services, and Have Taken Numerous Actions to Address Concerns Around Potential Misuse of Rekognition and Ring Products

Since introducing Amazon Rekognition, we have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, customer contractual requirements and training, consultation with third party experts, and other policies and practices. We understand the risks associated with potential misuse of facial recognition technology and, in connection with extensive discussions with customers, researchers, academics, policymakers, and civil society groups, we have taken the following actions to address concerns around potential misuse:

- *Implemented Police Moratorium.* In June 2020, AWS implemented a global moratorium on use of Amazon Rekognition's face comparison feature by police departments in connection with criminal investigations and, in May 2021, AWS announced the indefinite extension of that moratorium. In addition to our implementation of the moratorium on police use and legal terms for law enforcement use, AWS continues to engage with a large number of diverse stakeholders on these issues, including civil society groups, academia, policymakers, and law enforcement officials. As discussed below, we support appropriate legislative or regulatory frameworks to protect individual civil rights and ensure that governments

[4] See *https://www.aboutamazon.com/news/innovation-at-amazon/how-amazon-rekognition-helps-in-the-fight-against-some-of-the-worst-types-of-crime*.

are transparent in their use of facial recognition technology, and have consulted with and provided support to those working to address these issues.[5]

- *Actively Engage in Policy Discussions.* Amazon believes that facial recognition technology should not be banned or condemned simply because there is a potential that people may misuse it. Many technologies, like cell phones or cameras, could also be misused. Instead, as we have made clear in our statement of positions, "we think that governments and lawmakers should act to regulate the use of this technology to ensure it's used appropriately, and we have proposed guidelines for effective regulatory frameworks and guardrails that protect individual civil rights and ensures that governments are transparent in their application of the technology."[6]
- *Provide Customers with Responsible AI and Transparency Tools.* Our commitment to developing AI and ML in a responsible way is integral to how we build our services, engage with customers, and drive innovation. We are committed to providing customers with tools and resources to develop and use AI/ML responsibly. In November 2022, we launched AWS AI Service Cards, a new transparency resource to help customers better understand our AWS AI services, including one for Rekognition face matching.[7] AI Service Cards are a form of responsible AI documentation that provides customers with a single place to find information on the intended use cases and limitations, responsible AI design choices, and deployment and performance optimization best practices for our AI services. They are part of our evolving comprehensive development process we undertake to build our services in a responsible way that addresses fairness and bias, explainability, robustness, governance, transparency, privacy, and security in a state of the art manner. AI Service Cards will continue to evolve and expand as we engage with our customers and the broader community to gather feedback and continually iterate on our approach.
- *Dedicate Significant Resources to Machine Learning Accuracy and Bias Mitigation.* AWS dedicates significant resources to testing, auditing, and improving its technology so that it is constantly learning and improving accuracy, including providing diverse perspectives on its technology development teams, using training data sets that reflect gender, racial, ethnic, religious, and cultural diversity, and incorporating feedback from third parties. For example, Credo AI, a company that specializes in Responsible AI, performed a third-party evaluation of Rekognition using an identity verification dataset containing high-quality images of subjects with good lighting, no blur, and no occlusion. The evaluation supports our finding that Rekognition performs well across demographic attributes.[8] We have science and technical experts who help promote fairness in our products and services, including helping to design, test, and audit our services for fairness and accuracy and to mitigate potential bias, and who publish academic papers and provide thought leadership in this area. [9] AWS also makes available capabilities that help customers detect bias in ML models and increase transparency by helping explain model behavior to stakeholders and customers.[10] We continue to invest heavily in this area and work closely with customers and other stakeholders on addressing these important issues.
- *Support Standardized Testing Methodologies and Benchmarks.* We believe it is important that there be standardized testing methodologies and benchmarks for cloud-based facial recognition technologies. AWS encourages and supports the development of independent standards by entities like the National Institute of Standards and Technology (NIST) and other independent and recognized research organizations and standards bodies to develop tests that support cloud-based facial recognition software. We are engaging with NIST and other stakeholders to offer our direct assistance towards this effort. We also support efforts by members of the academic and commercial community to establish independent and trusted criteria, benchmarks, and evaluation protocols around facial recognition services.
- *Partner and Collaborate with External Stakeholders.* AWS collaborates with the academic community and other stakeholders on the responsible use of AI/ML technologies. For example, through our participation in Partnership on AI, we have worked with leading technology companies and organizations such as the ACLU, Future of Privacy Forum, and the MIT Initiative on the Digital Economy to advance public understanding of AI technologies and address opportunities and challenges with AI technologies to benefit people and society, focusing on areas such as ethics, fairness, inclusivity, and transparency. We are also active participants in other multi-stakeholder organizations relating to AI, including The Organisation for Economic Co-operation and Development (OECD) working groups on AI, the Global Partnership on AI,

---

5 Available at *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

6 Available at *https://www.aboutamazon.com/about-us/our-positions* and *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

7 See *https://aws.amazon.com/blogs/machine-learning/introducing-aws-ai-service-cards-a-new-resource-to-enhance-transparency-and-advance-responsible-ai/*.

8 See *https://aws.amazon.com/machine-learning/responsible-machine-learning/rekognition-face-matching/*.

9 Available at *https://arxiv.org/abs/2007.06570* (submitted Jul. 13, 2020), and *https://www.youtube.com/watch?v=JCGUYFe6P2k*. See also *https://www.amazon.science/blog/method-predicts-bias-in-face-recognition-models-using-unlabeled-data* (Nov. 8, 2022).

10 Available at *https://aws.amazon.com/sagemaker/clarify/*.

and the Responsible AI Institute. We also provide research grants through Amazon Research Awards and the joint Amazon and National Science Foundation Fairness in AI Grants program.

- *Require Customer Agreement to Acceptable Use Policy.* As a condition to using Amazon Rekognition and every other AWS service, a customer (including any government or law enforcement customer) must agree to the AWS Acceptable Use Policy (the "AUP"), which prohibits use of AWS's services "for any illegal or fraudulent activity."[11] This includes the violation of any laws related to privacy, discrimination, and civil rights. AWS will suspend or terminate access to Amazon Rekognition or any other AWS service if we determine a customer is violating our AUP or the AWS legal terms.
- *Enhanced Legal Terms.* All customers using any AWS service, including Amazon Rekognition, must comply with the relevant AWS legal terms. In early 2020, prior to our implementation of the moratorium on police use, we spent significant resources and consulted with law enforcement customers, civil society groups, and other stakeholders to perform an extensive review of and update to our legal terms to require certain disclosures and practices around law enforcement use cases. For example, if Amazon Rekognition is used to assist in identifying a person, and actions will be taken based on the identification that could impact that person's civil liberties or equivalent human rights, AWS legal terms require the decision to take action to be made by an appropriately trained person based on their independent examination of the identification evidence, and require the agency to ensure that such personnel receive appropriate training on the responsible use of facial recognition systems.[12] We believe this framework strikes a balance between the benefits and risks of use of facial recognition by law enforcement and helps address concerns around potential misuse.
- *Provide Customer Guidance on Best Practices and Acceptable Use.* AWS provides guidance to customers on best practices for utilizing and analyzing the results from using facial recognition technology. For example, in line with the AWS legal terms described above, AWS recommends that in public safety use cases human reviewers verify the system's results and decisions not be made based on the system output without additional human review. AWS also recommends customers be transparent about the use of face detection and comparison systems in such use cases, including, wherever possible, informing end users and subjects about the use of these systems, obtaining consent for that use, and providing a mechanism for end users and subjects to provide feedback to improve the system.[13] AWS also provides guidance to customers on the responsible design, deployment, and use of ML systems.[14] Further, customers can engage an AWS team of experts in responsible ML to recommend and help apply existing use-case-specific best practices on the development, deployment, and operationalization of responsible ML principles.[15] As noted above, we have cross-functional experts from engineering, science, product, legal, and policy backgrounds who establish processes and procedures to drive responsible use of AWS's AI/ML services, including Amazon Rekognition. When we are approached by or become aware of customers with potential use cases that may implicate our AUP, these experts analyze the proposed use case and we have turned down customers whose proposed uses would violate our AUP.
- *Provide Reporting Mechanisms.* AWS provides a website and e-mail address where any person can report suspected abuse, and AWS employs trained staff that review every report that is received. In the more than six years AWS has been offering Amazon Rekognition, AWS has not received a single verified report of Amazon Rekognition being used in the harmful manner posited in the proposal.

We have taken the following actions, among others, to limit potential misuse of Ring products and services:

- *Give Users Control and Innovate on Their Behalf.* The Neighbors App by Ring is a free application designed to help community members connect with each other and trusted sources of safety information like the public safety agencies that serve them. Ring designed Neighbors to protect user privacy and to keep users in control of what information, if any, they want to share. Users can choose whether or not to upload videos, photos, or text-based posts to Neighbors to publicly share safety-related information with their communities. Public safety agencies can only view publicly available content on Neighbors or videos that a user explicitly and voluntarily chooses to share with a public safety agency as part of an active investigation in response to a Request for Assistance ("RFA") post. Public safety agencies can use these posts to notify residents of an incident and ask their communities for help related to an investigation. RFA posts can easily be muted by users, and responses are entirely voluntary; nothing is shared with any agency in connection with an RFA post unless a user actively chooses to do so and Ring has no say or involvement in how a user may respond. The full text of

---

11 Available at *https://aws.amazon.com/aup/*.

12 See *https://aws.amazon.com/service-terms/*.

13 Available at *https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf*.

14 See *https://d1.awsstatic.com/responsible-machine-learning/responsible-use-of-machine-learning-guide.pdf*.

15 See *https://pages.awscloud.com/GLOBAL-aware-IND-AWS-ProServe-Responsible-ML-2021-reg.html*.

all RFA posts are publicly viewable in the Neighbors feed, and logged on the agency's public profile. Ring never provides police and other public safety officials access to device livestreams, control of user devices, or information on how many users viewed or muted an RFA post.

- *Audit with the NYU Policing Project and Continued Commitment to External Feedback.* In 2021, Ring completed a civil rights and civil liberties audit with the Policing Project at New York University School of Law to help Ring promote equity, transparency, and accountability in its products and services. The audit entailed nearly two years of work and was focused on potential racial justice, civil rights, civil liberties, and democratic accountability issues relating to both law enforcement's use of Neighbors and Ring's practices regarding law enforcement requests for information, including emergency requests for information. Based on recommendations and observations developed during the course of the audit, Ring implemented over one hundred changes to its products, policies, and legal processes, including introducing the public RFA post process.[16] This new post category, along with other changes such as adding community resources like mental health services to the Neighbors App, were cited by the Policing Project as steps Ring has taken to safeguard against improper use and address potential harms. Ring also actively solicits feedback on its products and services from independent experts, like the National Network to End Domestic Violence and the Center for Democracy and Technology (the "CDT"), to maintain different perspectives at the forefront of Ring's work.
- *Enforce Strict Limitations on Requests for Video Recordings.* Ring also imposes strict limitations on public safety agencies when they create a RFA post. For example, Ring's policy expressly prohibits agencies from creating a RFA post for lawful activities, such as protests, and the agencies must provide an active case or incident number related to a specific crime or safety incident before a RFA post can be viewed on user's feeds. Additional safeguards include: restricting local public safety agencies to only asking for videos recorded during a specified 12 hour period, such as noon to midnight, in a given day; requiring a minimum 0.025 square mile and maximum 0.5 square mile (approximately 10 city blocks) geographic region each time a public safety official asks for assistance to avoid targeting specific residents or broad geographic requests; prohibiting public safety officials from asking for video recordings more than 45 days after the incident under investigation took place; and requiring that public safety officials submit their request for assistance individually, not "batched." Ring moderates every post submitted before the post becomes available for viewing on Ring users' feeds to make sure it follows our guidelines, and Ring does not allow for open requests for footage.
- *Require Customer Agreement to Community Guidelines.* Ring is committed to upholding a standard of trust and civility and does not tolerate racial profiling, hate speech, and other forms of profiling or prejudice on Neighbors. Ring requires all Neighbors users, including public safety and local government agencies, to agree to strict community guidelines, which prohibit racial profiling, hate speech, and other forms of discrimination. Ring has a dedicated group of team members, who are trained regarding critical and timely issues, proactively moderating Neighbors content and working to remove prohibited content prior to posting publicly, 24 hours a day, seven days a week. When posts are denied, an email is sent to the Neighbors user who submitted the post to inform them of the reason, reinforcing our guidelines and helping users make responsible decisions. In addition, Neighbors users can flag incorrect or inappropriate content directly in the App. The moderation team will remove the flagged content if they determine that the content violates community guidelines. Ring also engaged the CDT to provide counsel and help strengthen its moderation practices, and the CDT contributed to updates to the Neighbors App and community guidelines in 2021 and continues to provide feedback to Ring today.
- *Share Clear Law Enforcement Guidelines*. Like any other company, Ring is obligated to review and respond to legally binding requests for information from law enforcement. Ring does not disclose customer information to law enforcement in connection with government demands unless we are compelled to do so to comply with law (i.e., legally valid and binding requests for information from law enforcement agencies such as search warrants signed by a judge, subpoenas, and court orders). Ring carefully reviews each of these requests and challenges those that we believe to be overbroad or otherwise inappropriate. As part of the NYU Policing Project audit, Ring updated its law enforcement information request reporting to share the type and number of binding information requests processed on a biannual basis.[17] Like many other companies, on rare occasions Ring may provide information to law enforcement on an emergency basis when there is an imminent danger of death or serious physical injury, such as a kidnapping or an attempted murder. Ring has robust policies and practices for evaluating these requests. Trained members of the legal team carefully review these submissions and emergency requests are regularly denied. These policies have long been reflected in Ring's public-facing Law Enforcement Guidelines, Terms of Service, and Privacy Notice.
- *Deliver on Privacy and Security Commitment.* Ring continues to innovate and identify new ways to help uphold customer privacy and security and give users even more control over their devices and personal information. For example, Ring

[16] For more information on the Policing Project's civil rights and civil liberties audit, see *https://www.policingproject.org/ring*.

[17] See *https://ring.com/law-enforcement-information-requests*.

launched video end-to-end encryption for non-battery powered cameras and doorbells in the United States in early 2021, a feature that allows customers to further secure their videos with an additional virtual lock, which can only be unlocked by a key that is stored on the customer's enrolled mobile device, designed so that only the customer can decrypt and view recordings on their enrolled device. In 2022, Ring expanded support for video end-to-end encryption to most of its battery-powered camera and doorbell devices, and to additional countries outside of the United States.

Our Board has reviewed Amazon Rekognition, along with many other programs, as part of numerous AWS business reviews, and has also reviewed Ring over the course of several meetings since our acquisition of Ring. In addition, our Nominating and Corporate Governance Committee has provided oversight on behalf of the Board over the human rights aspects of Amazon's Rekognition technology and Ring, as well as our other technologies, and has specifically reviewed Amazon Rekognition's facial recognition capabilities and Ring. These reviews focus on the actual operation and use of Amazon Rekognition and Ring, the potential concerns and abuses that critics have suggested could arise from these technologies, and our actions to resolve or mitigate those risks and concerns. Under its charter, the Nominating and Corporate Governance Committee, which is comprised of directors with experience in emerging technologies and public policy, is given responsibility for overseeing and monitoring the Company's policies and initiatives relating to corporate social responsibility, including human rights and ethical business practices, and risks related to the Company's operations and engagement with customers, suppliers, and communities.

This Proposal Fails to Acknowledge or Address the Measures We Have Taken to Enhance Our Technology and Relies on Dated Claims and Mischaracterizations

While we have been working to constantly enhance our AI/ML technology, including Amazon Rekognition and Ring products and services, and have avoided or mitigated the risks and concerns posited in this proposal, this proposal has relied on the same outdated assertions and mischaracterizations. For example, this proposal continues to incorrectly insinuate that Amazon Rekognition is a surveillance program. In fact, Amazon Rekognition, does not collect images for users to perform searches on and does not provide any photos or data for users to search or compare images against. Instead, the service can be used to help identify objects, people, text, scenes, and activities in images and videos, as well as to detect inappropriate content. In addition, this proposal dismisses the Policing Project's civil rights and civil liberties audit and the review and feedback Ring received from the CDT, and uses vague innuendo or mischaracterizations to suggest concerns with the operation of our policies and our products. We believe our actions demonstrate that we are willing to work constructively to address realistic issues and work toward solutions that continue to allow customers to benefit from useful technologies, while the proponents of this proposal appear unwilling to acknowledge any action as sufficient.

The proposal requests that the Company prepare a report about Amazon's process for customer due diligence to determine whether customers' use of certain of our products or services contributes to human rights violations. Conversations around responsible development and use of AI/ML systems are happening around the world among government, industry, academia, and other groups. Amazon is an active participant and contributor to these conversations, and Amazon teams and subject matter experts are helping lead the industry on these very issues. As demonstrated above, we have conscientiously acted to review and address the concerns expressed in the proposal and transparently provided information regarding our actions to the public. In light of our commitment to customer trust, privacy, and security; the material benefits to both society and organizations of Amazon's technology products and services; and our ongoing transparency and efforts to address potential misuse of those products and services, the Board recommends that shareholders vote against this proposal.

The Board of Directors recommends a vote "AGAINST" this proposal requesting a report on customer due diligence.

EXHIBIT D

ITEM 6—SHAREHOLDER PROPOSAL REQUESTING A REPORT ON CUSTOMER DUE DILIGENCE

Beginning of Shareholder Proposal and Statement of Support:

Customer Due Diligence

2022 - Amazon.com, Inc.

Resolved: Shareholders request the Board of Directors commission an independent third-party report, at reasonable cost and omitting proprietary information, assessing Amazon's customer due diligence process to determine whether customers' use of its products and services with surveillance, computer vision, or cloud storage capabilities contributes to human rights violations.

Whereas: Amazon Web Services (AWS) is a leading cloud provider that serves multiple government customers with a history of human rights abuses, and Amazon's surveillance technologies may enable mass surveillance globally.

"Know Your Customer" due diligence mitigates clients' risks and human rights impacts and informs business decision-making.[1] It reveals whether technologies will be used to facilitate governmental human or civil rights or civil liberties violations.[2] The Atlantic Council recommended the United States and NATO "create know-your-customer (KYC) policies" with surveillance companies.[3] The United Nations found that states and businesses have "often rushed to incorporate AI applications, failing to carry out due diligence."[4]

Inadequate due diligence presents material privacy and data security risks, as well as legal, regulatory, and reputational risks. These risks are present even if surveillance products are used according to Amazon's guidelines. Amazon fails to address how its facial analysis products enable discrimination.[5] Even after police used Amazon's Ring to surveil anti-racist protesters[6] and a UK court found Ring infringed customer privacy,[7] Ring continues to expand its thousands of police partnerships.[8] Senators expressed concerns[9] that Amazon's palm recognition payment system violates privacy.[10] In 2021, Amazon was fined $887 million for violating the European Union General Data Protection Regulation.[11]

Amazon's government and government-affiliated customers and suppliers with a history of rights-violating behavior pose risks to the company, including:

- U.S. immigration enforcement agencies use AWS in detention and deportation programs;
- AWS will host the Department of Homeland Security's biometric database, which will impact millions of immigrants' and citizens' "ability to exercise their rights to protest, assemble, associate, and to live their daily lives";
- Amazon has purchased thermal cameras from Chinese technology firm Dahua,[12] which was blacklisted by the U.S. Government due to its role in the mass surveillance, internment, torture, and forced labor of the ethnic Uyghur minority;
- The Israeli military and government's "Project Nimbus", protested by Amazon employees,[13] uses AWS to support and expand the apartheid system under which Palestinians in occupied territory are surveilled, unlawfully detained and tortured, and subjected to acts of forced displacement.[14] The Israel Land Authority plans to use AWS as it expands illegal settlements and enforces segregation; and
- The United Arab Emirates government, which deploys a state surveillance apparatus against human rights defenders, journalists, and political dissidents, will partner with Amazon to develop three data centers in 2022.

Amazon's existing policies[15] appear insufficient in preventing customer misuse and establishing effective oversight, yet Amazon continues releasing surveillance products.

---

1 https://www.humanrights.dk/sites/humanrights.dk/files/media/document/Phase%204_%20Impact%20prevent

2 https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic

3 https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf

4 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E

5 https://venturebeat.com/2021/09/03/bias-persists-in-face-detection-systems-from-amazon-microsoft-and-google/

6 https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests

7 https://www.digitalcameraworld.com/news/your-amazon-ring-camera-could-land-you-in-trouble-with-the-law-after-shock-ruling

8 https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras

9 https://www.klobuchar.senate.gov/public/_cache/files/5/e/5ebfd9e0-b230-4a86-8db4-09cacd0c25a6/0DA3E8409AD9EB20E056BC005E5858B1.8.12.21-letter-to-amazon.pdf

10 https://news.sky.com/story/amazon-introduces-palm-swiping-technology-to-concert-venue-in-us-12407679

11 https://www.theverge.com/2021/7/30/22601661/amazon-gdpr-fine-cnpd-marketplace-antitrust-data

12 https://www.theguardian.com/technology/2020/apr/29/amazon-thermal-cameras-china-dahua

13 https://www.theguardian.com/commentisfree/2021/oct/12/google-amazon-workers-condemn-project-nimbus-israeli-military-contract

14 https://www.un.org/unispal/wp-content/uploads/2020/06/AHRC43NGO185.pdf ; https://www.hrw.org/report/2021/04/27/threshold-crossed/israeli-authorities-and-crimes-apartheid-and-persecution#

15 https://sustainability.aboutamazon.com/people/human-rights/principles ; https://ir.aboutamazon.com/corporate-governance/documents-and-charters/code-of-business-conduct-and-ethics/default.aspx ; https://aws.amazon.com/agreement/

End of Shareholder Proposal and Statement of Support

RECOMMENDATION OF THE BOARD OF DIRECTORS ON ITEM 6

Why We Recommend You Vote Against This Proposal

- Amazon's technology products and services can be used to solve complex problems that benefit society. Since being introduced in 2016, non-profit, advocacy, and government groups have used Amazon Rekognition's facial recognition capabilities to protect human rights, including tracking and stopping child exploitation and rescuing victims of human trafficking, as well as locating hundreds of missing children. Similarly, Ring strives to fulfill its mission to make neighborhoods safer, including by inventing home security products that solve real customer problems and by assisting community members in sharing important safety information and connecting with each other.
- Amazon is committed to the responsible use of our artificial intelligence and machine learning (AI/ML) products and services. We have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, customer contractual requirements and training, consultation with third party experts, and other policies and practices. We have implemented a moratorium on police use of Amazon Rekognition's facial comparison feature for criminal investigations. We believe this moratorium will give governments time to implement appropriate rules, and we stand ready to help with any such initiatives. As part of a commitment to improving its products and services by listening to feedback from community stakeholders and independent experts, Ring has conducted a civil rights and civil liberties audit with the Policing Project at New York University School of Law.
- While we have been updating our technology and enhancing safeguards, this proposal has recited the same years-old claims and mischaracterizations, even though in the more than five years AWS has been offering Amazon Rekognition AWS has never received a report of Amazon Rekognition being misused in the manner posited in this proposal. Contrary to the proponent's mischaracterization, it is not a surveillance system.

Amazon's Technology Products and Services Have the Capability to Solve Complex Problems and Benefit Society

When used properly and responsibly, the technology products and services offered by Amazon provide material benefits to society and the communities and organizations that use them. For example, since being introduced in 2016, non-profit, advocacy, and government groups have used Amazon Rekognition's facial recognition capabilities to protect human rights, including tracking and stopping child exploitation and rescuing victims of human trafficking, as well as locating hundreds of missing children. It has also been used to build educational apps, enhance security through multi-factor authentication, identify suggestive or explicit website content in order to block or remove those images, and provide identity verification as part of mobile banking services for underbanked individuals in emerging geographies. Similarly, Ring strives to fulfill its mission to make neighborhoods safer, including by inventing home security products that solve real customer problems and assisting community members in sharing important safety information and connecting with each other. These are just a few of the numerous beneficial applications of these technologies.

We Are Committed to the Responsible Use of Our AI/MI Products and Services and Have Taken Numerous Actions to Address Concerns Around Potential Misuse of Rekognition and Ring Products

Since introducing Amazon Rekognition, we have been consistent and proactive in our efforts to address concerns and mitigate the risk of misuse through policy and advocacy efforts, customer contractual requirements and training, consultation with third party experts, and other policies and practices. We understand the risks associated with potential misuse of facial recognition technology and, in connection with extensive discussions with customers, researchers, academics, policymakers, and civil society groups, we have taken the following actions to review and address concerns around potential misuse:

- *Implemented Police Moratorium.* In June 2020, AWS implemented a moratorium on use of Amazon Rekognition's face comparison feature by police departments in connection with criminal investigations and, in May 2021, AWS announced the indefinite extension of that moratorium. We believe this moratorium will give governments time to implement appropriate rules, and we stand ready to help with any such initiatives. Since this announcement, several United States state and local jurisdictions have introduced, debated, and implemented such laws, and we anticipate additional activity and progress in this area. We support the calls for an appropriate national legislative framework that protects individual civil rights and ensures that governments are transparent in their use of facial recognition technology, and have provided guidance to those thinking about these issues.[6]
- *Actively Engage in Policy Discussions.* Amazon believes that facial recognition technology should not be banned or condemned simply because there is a potential that people may misuse it. Many technologies, like cell phones or cameras, could also be misused. Instead, as we have made clear in our statement of positions, "we think that governments and lawmakers should act to regulate the use of this technology to ensure it's used appropriately, and we have proposed guidelines for effective regulatory frameworks and guardrails that protect individual civil rights and ensures that governments are transparent in their application of the technology."[7] In addition to our implementation of the moratorium on police use and legal terms for law enforcement use, AWS continues to engage with a large number of diverse stakeholders on these issues, including civil society groups, academia, policymakers, and law enforcement officials.
- *Dedicate Significant Resources to Machine Learning Accuracy and Bias Mitigation.* AWS dedicates significant resources to testing, auditing, and improving its technology so that it is constantly learning and improving accuracy, including providing diverse perspectives on its technology development teams, using training data sets that reflect gender, racial, ethnic, religious, and cultural diversity, and incorporating feedback from third parties. We have science and technical experts who help promote fairness in our products and services, including helping to design, test, and audit our services for fairness and accuracy and to mitigate potential bias, and who publish academic papers and provide thought leadership in this area.[8] AWS also makes available capabilities that help customers detect bias in ML models and increase transparency by helping explain model behavior to stakeholders and customers.[9] We continue to invest heavily in this area and work closely with customers and other stakeholders on addressing these important issues.
- *Support Standardized Testing Methodologies and Benchmarks.* We believe it is important that there be standardized testing methodologies and benchmarks for cloud-based facial recognition technologies. AWS encourages and supports the development of independent standards by entities like the National Institute of Standards and Technology (NIST) and other independent and recognized research organizations and standards bodies to develop tests that support cloud-based facial recognition software. We are engaging with NIST and other stakeholders to offer our direct assistance towards this effort. We also support efforts by members of the academic community to establish independent and trusted criteria, benchmarks, and evaluation protocols around facial recognition services.
- *Partner and Collaborate with External Stakeholders*. AWS collaborates with the academic community and other stakeholders on the responsible use of AI/ML technologies. For example, through our participation in Partnership on AI, we have worked with leading technology companies and organizations such as the ACLU, Future of Privacy Forum, and the MIT Initiative on the Digital Economy to advance public understanding of AI technologies and address opportunities and challenges with AI technologies to benefit people and society, focusing on areas such as ethics, fairness, inclusivity, and transparency. We are also active members of other multi-stakeholder organizations relating to AI, including The

6 Available at *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

7 Available at *https://www.aboutamazon.com/about-us/our-positions* and *https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/*.

8 Available at *https://arxiv.org/abs/2007.06570* and *https://www.youtube.com/watch?v=JCGUYFe6P2k*.

9 Available at *https://aws.amazon.com/sagemaker/clarify/*.

Organisation for Economic Co-operation and Development (OECD) working groups on AI. We also provide research grants through Amazon Research Awards and the joint Amazon and National Science Foundation Fairness in AI Grants program.

- *Require Customer Agreement to Acceptable Use Policy.* As a condition to using Amazon Rekognition and every other AWS service, a customer (including government or law enforcement customers) must accept the AWS Acceptable Use Policy (the "AUP"), which prohibits use of AWS's services "for any illegal or fraudulent activity."[10] This includes the violation of any laws related to privacy, discrimination, and civil rights. AWS will suspend or terminate access to Amazon Rekognition if we determine a customer is violating our AUP or the AWS legal terms.
- *Enhanced Legal Terms.* All customers using Amazon Rekognition must comply with the relevant AWS legal terms. In early 2020, prior to our implementation of the moratorium on police use, we spent significant resources and consulted with law enforcement customers, civil society groups, and other stakeholders to perform an extensive review of and update to our legal terms to require certain disclosures and practices around law enforcement use cases. For example, if a law enforcement agency uses Amazon Rekognition in connection with criminal investigations, AWS legal terms require it to publicly disclose its use of facial recognition systems, summarize the safeguards in place to prevent violations of civil liberties or equivalent human rights, and make the disclosure easily accessible; we also direct customers to resources made available by the U.S. Federal Bureau of Investigation and Department of Justice in this area.[11] In addition, if Amazon Rekognition is used to assist in identifying a person, and actions will be taken based on the identification that could impact that person's civil liberties or equivalent human rights, AWS legal terms require the decision to take action to be made by an appropriately trained person based on their independent examination of the identification evidence, and require the agency to ensure that such personnel receive appropriate training on the responsible use of facial recognition systems.[12] We believe this framework strikes a balance between the benefits and risks of use of facial recognition by law enforcement and helps address concerns around potential misuse.
- *Provide Customer Guidance on Best Practices and Acceptable Use.* AWS provides guidance to customers on best practices for utilizing and analyzing the results from using facial recognition technology. For example, in line with the AWS legal terms described above, AWS recommends that in public safety use cases human reviewers verify the system's results and decisions not be made based on the system output without additional human review. AWS also recommends customers be transparent about the use of face detection and comparison systems in such use cases, including, wherever possible, informing end users and subjects about the use of these systems, obtaining consent for that use, and providing a mechanism for end users and subjects to provide feedback to improve the system.[13] AWS also provides guidance to customers on the responsible design, deployment, and use of ML systems.[14] Further, customers can engage an AWS team of experts in responsible ML to recommend and help apply existing use-case-specific best practices on the development, deployment, and operationalization of responsible ML principles.[15] As noted above, we have cross-functional experts from engineering, science, product, legal, and policy backgrounds who establish processes and procedures to drive responsible use of AWS's AI/ML services, including Amazon Rekognition. When we are approached by or become aware of customers with potential use cases that may implicate our AUP, these experts analyze the proposed use case and we have turned down customers whose proposed uses would violate our AUP.
- *Provide Reporting Mechanisms.* AWS provides a website and e-mail address where any person can report suspected abuse, and AWS employs trained staff that review every report that is received. In the more than five years AWS has been offering Amazon Rekognition, AWS has not received a single report of Amazon Rekognition being used in the harmful manner posited in the proposal.

We have taken the following actions, among others, to limit potential misuse of Ring products and services:

- *Allow Users to Choose What to Share.* The Neighbors App by Ring is a free application designed to help community members connect with each other and trusted sources of safety information like the public safety agencies that serve

---

10 Available at *https://aws.amazon.com/aup/*.

11 See *https://aws.amazon.com/service-terms/* (Section 50.8.4). This term directs customers to example FBI statements, FBI privacy assessments, and the Facial Recognition Policy Development Template published by the U.S Department of Justice's Bureau of Justice Assistance; see also *https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use*; *https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit*; *https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf*.

12 See *https://aws.amazon.com/service-terms/*.

13 Available at *https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf*.

14 See *https://d1.awsstatic.com/responsible-machine-learning/responsible-use-of-machine-learning-guide.pdf*.

15 See *https://pages.awscloud.com/GLOBAL-aware-IND-AWS-ProServe-Responsible-ML-2021-reg.html*.

them. Ring designed Neighbors to protect user privacy and to keep users in control of what information, if any, they want to share. Users can choose to upload videos, photos, or text-based posts to Neighbors to publicly share crime and safety-related information with their communities. They can also choose not to do that. With Neighbors, public safety agencies can only view publicly available content on Neighbors or videos that a user explicitly and voluntarily chooses to share with a public safety agency as part of an active investigation. Police and other public safety officials do not have access to users' devices, device locations, video recordings, or personal information when using Neighbors unless a user chooses to share. Ring never provides police and other public safety officials access to device livestreams.

- *Audit with the NYU Policing Project.* In 2021, Ring completed a civil rights and civil liberties audit with the Policing Project at New York University School of Law. The audit represented nearly two years of work and was focused on potential racial justice, civil rights, civil liberties, and democratic accountability issues relating to law enforcement's use of Neighbors and Ring's practices regarding law enforcement requests for information. As part of the audit, the Policing Project presented Ring with a detailed set of recommendations. During the course of the audit, Ring implemented over one hundred changes to its products, policies, and legal processes. For example, public safety agencies are now only able to request information or video from their communities through a new, publicly viewable post category on Neighbors called Request for Assistance. Public safety agencies can use these posts to notify residents of an incident and ask their communities for help related to an investigation. The full text of all Request for Assistance posts are publicly viewable in the Neighbors feed, and logged on the agency's public profile. This way, anyone interested in knowing more about how an agency is using Request for Assistance posts can simply visit the agency's profile and see the post history. Request for Assistance posts are opt-in; nothing is shared with any agency unless a user actively chooses to do so. Users can also remove Request for Assistance posts from their feed. Public safety agencies are not able to see how many users viewed a Request for Assistance post or which users removed those posts from their feed.[16] This new post category, along with other changes such as adding community resources like mental health services to the Neighbors App, were cited by the Policing Project as steps Ring has taken to safeguard against improper use and address potential harms.
- *Enforce Strict Limitations on Requests for Video Recordings.* Ring also imposes strict limitations on public safety agencies when they create a Request for Assistance post. For example, Ring's policy expressly prohibits agencies from creating a Request for Assistance post for lawful activities, such as protests, and the agencies must provide an active case or incident number related to a specific crime or safety incident before a Request for Assistance post can be viewed on user's feeds. Additional safeguards include: restricting local public safety agencies to only asking for videos recorded during a specified 12 hour period, such as noon to midnight, in a given day; requiring a minimum 0.025 square mile and maximum 0.5 square mile (approximately 10 city blocks) geographic region each time a public safety official asks for assistance to avoid targeting specific residents or broad geographic requests; prohibiting public safety officials from asking for video recordings more than 45 days after the incident under investigation took place; and requiring that public safety officials submit their request for assistance individually, not "batched." Ring moderates every post submitted before the post becomes available for viewing on Ring users' feeds to make sure it follows our guidelines, and Ring does not allow for open requests for footage.
- *Require Customer Agreement to Community Guidelines.* Ring is committed to upholding a standard of trust and civility and does not tolerate racial profiling, hate speech, and other forms of profiling or prejudice on Neighbors. Ring requires all Neighbors users to agree to strict community guidelines, which prohibit racial profiling, hate speech, and other forms of discrimination. To monitor compliance with these standards, Ring also invests heavily in manual and automated content moderation. Ring has a dedicated group of team members, who are trained regarding critical and timely issues, proactively moderating Neighbors content and working to remove prohibited content prior to posting publicly, 24 hours a day, seven days a week. When posts are denied, an email is sent to the Neighbors user who submitted the post to inform them of the reason, reinforcing our guidelines and helping users make responsible decisions. In addition, Neighbors users can flag incorrect or inappropriate content directly in the App. The moderation team will remove the flagged content if they determine that the content violates community guidelines. Ring also engaged the Center for Democracy and Technology (the "CDT") to provide counsel and help strengthen its moderation practices, and the CDT contributed to updates to the Neighbors App and community guidelines in 2021.
- *Deliver on Privacy and Security Commitment.* Ring continues to innovate and identify new ways to help uphold customer privacy and security and give users even more control over their devices and personal information. For example, Ring launched end-to-end encryption in early 2021, a feature that allows customers to further secure their videos with an additional virtual lock, which can only be unlocked by a key that is stored on the customer's enrolled mobile device, designed so that only the customer can decrypt and view recordings on their enrolled device.

[16] For more information on the Policing Project's civil rights and civil liberties audit, see *https://www.policingproject.org/ring*.

Our Board has reviewed Amazon Rekognition, along with many other programs, as part of numerous AWS business reviews, and has also reviewed Ring in several of its meetings since our acquisition of Ring. In addition, our Nominating and Corporate Governance Committee has provided oversight on behalf of the Board over the human rights aspects of Amazon's Rekognition technology and Ring, as well as our other technologies, and has specifically reviewed Amazon Rekognition's facial recognition capabilities and Ring. These reviews focus on the actual operation and use of Amazon Rekognition and Ring, the potential concerns and abuses that critics have suggested could arise from these technologies, and our actions to resolve or mitigate those risks and concerns. Under its charter, the Nominating and Corporate Governance Committee, which is comprised of directors with experience in emerging technologies and public policy, is given responsibility for overseeing and monitoring the Company's policies and initiatives relating to corporate social responsibility, including human rights and ethical business practices, and risks related to the Company's operations and engagement with customers, suppliers, and communities.

This Proposal Fails to Acknowledge or Address the Measures We Have Taken to Enhance Our Technology and Relies on Dated Claims and Mischaracterizations

While we have been working to constantly enhance our AI/ML technology, including Amazon Rekognition and Ring products and services, this proposal has relied on the same outdated assertions and mischaracterizations. For example, this proposal continues to mischaracterize Amazon Rekognition as a surveillance program. In fact, Amazon Rekognition, does not collect images for users to perform searches on and does not provide any photos or data for users to search or compare images against. Instead, the service can be used to help identify objects, people, text, scenes, and activities in images and videos, as well as to detect inappropriate content. Similarly, the Proposal fails to acknowledge the improvements we have implemented for Ring as part of the Policing Project's civil rights and civil liberties audit and an ongoing commitment to innovate on behalf of customers and their communities.

The proposal requests that the Company prepare a report about Amazon's process for customer due diligence to determine whether customers' use of certain of our products or services contributes to human rights violations. Conversations around responsible development and use of AI/ML systems are happening around the world among government, industry, academia, and other groups. Amazon is an active participant and contributor to these conversations, and Amazon teams and subject matter experts are helping lead the industry on these very issues. As demonstrated above, we have conscientiously acted to review and address the concerns expressed in the proposal and transparently provided information regarding our actions to the public. In light of our commitment to customer trust, privacy, and security; the material benefits to both society and organizations of Amazon's technology products and services; and our ongoing transparency and efforts to address potential misuse of those products and services, the Board recommends that shareholders vote against this proposal.

The Board of Directors recommends a vote "AGAINST" this proposal requesting a report on customer due diligence.

ITEM 7—SHAREHOLDER PROPOSAL REQUESTING AN ALTERNATIVE DIRECTOR CANDIDATE POLICY

Beginning of Shareholder Proposal and Statement of Support:

Policy to Include Hourly Employees as Director Candidates

RESOLVED: Shareholders of Amazon.com, Inc. ("Amazon") urge the board to adopt a policy of promoting significant representation of employee perspectives among corporate decision makers by requiring that the initial list of candidates from which new board nominees are chosen (the "Initial List") by the Nominating and Governance Committee include (but need not be limited to) hourly employees. The policy should provide that any third-party consultant asked to furnish an Initial List will be requested to include such candidates.

WHEREAS: Amazon has been publicly excoriated for mistreating workers—including criticism over dehumanizing working conditions, anti-union activities, and straining taxpayers by paying so little that employees must rely on food stamps.[1] Employees have described workplace conditions as "hellish,"[2] and the NY Times observes that during the pandemic, "Amazon's system burned through workers, resulted in inadvertent firings and stalled benefits, and impeded communication, casting a shadow over a business success story for the ages."[3] Because protecting the company's reputation and ability to retain its

EXHIBIT E

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 8-K

CURRENT REPORT

Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934

May 22, 2024
Date of Report
(Date of earliest event reported)

AMAZON.COM, INC.

(Exact name of registrant as specified in its charter)

Delaware	**000-22513**	**91-1646860**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

410 Terry Avenue North, Seattle, Washington 98109-5210
(Address of principal executive offices, including Zip Code)

(206) 266-1000
(Registrant's telephone number, including area code)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	**Trading Symbol(s)**	**Name of Each Exchange on Which Registered**
Common Stock, par value $.01 per share	AMZN	Nasdaq Global Select Market

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

TABLE OF CONTENTS

ITEM 5.07. SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS.

On May 22, 2024, Amazon.com, Inc. (the "Company") held its Annual Meeting of Shareholders.

The following nominees were elected as directors, each to hold office until the next Annual Meeting of Shareholders or until his or her successor is elected and qualified, by the vote set forth below:

Nominee	For	Against	Abstain	Broker Non-Votes
Jeffrey P. Bezos	7,178,428,474	395,520,419	18,362,522	1,260,267,192
Andrew R. Jassy	7,467,074,640	104,919,757	20,317,018	1,260,267,192
Keith B. Alexander	7,488,855,654	84,451,453	19,004,308	1,260,267,192
Edith W. Cooper	7,117,067,591	456,429,050	18,814,774	1,260,267,192
Jamie S. Gorelick	7,262,009,164	310,078,904	20,223,347	1,260,267,192
Daniel P. Huttenlocher	7,374,651,006	198,658,047	19,002,362	1,260,267,192
Andrew Y. Ng	7,529,032,996	44,719,360	18,559,059	1,260,267,192
Indra K. Nooyi	7,458,579,786	115,442,726	18,288,903	1,260,267,192
Jonathan J. Rubinstein	6,730,127,279	841,312,680	20,871,456	1,260,267,192
Brad D. Smith	7,532,095,432	41,132,053	19,083,930	1,260,267,192
Patricia Q. Stonesifer	7,205,090,201	368,713,118	18,508,096	1,260,267,192
Wendell P. Weeks	7,469,871,725	103,122,974	19,316,716	1,260,267,192

The appointment of Ernst & Young LLP as our independent auditors for the fiscal year ending December 31, 2024 was ratified by the vote set forth below:

For	Against	Abstain	Broker Non-Votes
8,411,003,684	419,855,909	21,719,014	—

The compensation of our named executive officers as disclosed in the proxy statement was approved in an advisory vote, as set forth below:

For	Against	Abstain	Broker Non-Votes
5,878,960,949	1,687,781,127	25,569,339	1,260,267,192

A shareholder proposal requesting an additional board committee to oversee public policy was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
490,254,237	6,930,488,473	171,568,705	1,260,267,192

A shareholder proposal requesting an additional board committee to oversee the financial impact of policy positions was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
44,166,069	7,411,690,128	136,455,218	1,260,267,192

A shareholder proposal requesting a report on customer due diligence was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
1,248,281,806	6,184,374,303	159,655,306	1,260,267,192

A shareholder proposal requesting additional reporting on lobbying was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
2,240,780,384	5,302,796,026	48,735,005	1,260,267,192

A shareholder proposal requesting additional reporting on gender/racial pay was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
2,221,121,179	5,338,238,279	32,951,957	1,260,267,192

A shareholder proposal requesting a report on viewpoint restriction was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
58,637,628	7,479,861,945	53,811,842	1,260,267,192

A shareholder proposal requesting additional reporting on stakeholder impacts was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
1,764,453,585	5,774,937,195	52,920,635	1,260,267,192

A shareholder proposal requesting a report on packaging materials was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
2,160,008,116	5,381,900,903	50,402,396	1,260,267,192

A shareholder proposal requesting additional reporting on freedom of association was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
2,398,484,693	5,141,991,512	51,835,210	1,260,267,192

A shareholder proposal requesting alternative emissions reporting was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
1,148,925,070	6,385,459,156	57,927,189	1,260,267,192

A shareholder proposal requesting a report on customer use of certain technologies was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
1,436,306,088	6,092,329,924	63,675,403	1,260,267,192

A shareholder proposal requesting a policy to disclose directors' political and charitable donations was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
76,686,634	7,483,638,673	31,986,108	1,260,267,192

A shareholder proposal requesting an additional board committee to oversee artificial intelligence was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
729,956,170	6,791,566,706	70,788,539	1,260,267,192

A shareholder proposal requesting a report on warehouse working conditions was not approved, as set forth below:

For	Against	Abstain	Broker Non-Votes
2,356,031,178	5,185,496,222	50,784,015	1,260,267,192

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

AMAZON.COM, INC. (REGISTRANT)

By: /s/ Mark F. Hoffman
Mark F. Hoffman
Vice President and Secretary

Dated: May 24, 2024